特 許 協 力 条 約

PCT

特許性に関する国際予備報告（特許協力条約第二章）

（法第12条、法施行規則第56条）
〔ＰＣＴ36条及びＰＣＴ規則70〕

出願人又は代理人の書類記号 WN-2735P	今後の手続きについては、様式ＰＣＴ／ＩＰＥＡ／４１６を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ２００５／００１４３７	国際出願日 （日．月．年） ２６．０１．２００５	優先日 （日．月．年） ２６．０１．２００４
国際特許分類（ＩＰＣ） Int.Cl. *G09C1/00 (2006.01)*		
出願人（氏名又は名称） 日本電気株式会社		

１．この報告書は、ＰＣＴ35条に基づきこの国際予備審査機関で作成された国際予備審査報告である。
法施行規則第57条（ＰＣＴ36条）の規定に従い送付する。

２．この国際予備審査報告は、この表紙を含めて全部で 3 ページからなる。

３．この報告には次の附属物件も添付されている。

a．☑ 附属書類は全部で 5 ページである。

☑ 補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関が認めた訂正を含む明細書、請求の範囲及び／又は図面の用紙（ＰＣＴ規則70.16及び実施細則第607号参照）

☐ 第Ｉ欄４．及び補充欄に示したように、出願時における国際出願の開示の範囲を超えた補正を含むものとこの国際予備審査機関が認定した差替え用紙

b．☐ 電子媒体は全部で ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿（電子媒体の種類、数を示す）。
配列表に関する補充欄に示すように、電子形式による配列表又は配列表に関連するテーブルを含む。
（実施細則第802号参照）

４．この国際予備審査報告は、次の内容を含む。

☑ 第Ｉ欄 国際予備審査報告の基礎
☐ 第Ⅱ欄 優先権
☐ 第Ⅲ欄 新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成
☐ 第Ⅳ欄 発明の単一性の欠如
☑ 第Ⅴ欄 ＰＣＴ35条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明
☐ 第Ⅵ欄 ある種の引用文献
☐ 第Ⅶ欄 国際出願の不備
☐ 第Ⅷ欄 国際出願に対する意見

国際予備審査の請求書を受理した日 １９．０８．２００５	国際予備審査報告を作成した日 １７．０２．２００６
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） ５Ｓ ３５７４ 石川 正二 電話番号 ０３－３５８１－１１０１ 内線 ３５４６

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（２００５年４月）

特許性に関する国際予備報告

国際出願番号 PCT／JP2005／001437

第Ⅰ欄 報告の基礎

1．言語に関し、この予備審査報告は以下のものを基礎とした。

☑ 出願時の言語による国際出願

☐ 出願時の言語から次の目的のための言語である＿＿＿＿＿＿ 語に翻訳された、この国際出願の翻訳文

☐ 国際調査（ＰＣＴ規則12.3(a)及び23.1(b)）
☐ 国際公開（ＰＣＴ規則12.4(a)）
☐ 国際予備審査（ＰＣＴ規則55.2(a)又は55.3(a)）

2．この報告は下記の出願書類を基礎とした。（法第6条（ＰＣＴ14条）の規定に基づく命令に応答するために提出された差替え用紙は、この報告において「出願時」とし、この報告に添付していない。）

☐ 出願時の国際出願書類

☑ 明細書

第 1-81 ページ、出願時に提出されたもの
第＿＿＿＿ ページ*、＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿ ページ*、＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 請求の範囲

第 5-10 項、出願時に提出されたもの
第＿＿＿＿ 項*、ＰＣＴ１９条の規定に基づき補正されたもの
第 1-3 項*、19.08.2005 付けで国際予備審査機関が受理したもの
第＿＿＿＿ 項*、＿＿＿＿ 付けで国際予備審査機関が受理したもの

☑ 図面

第 1-17 ページ／図、出願時に提出されたもの
第＿＿＿＿ ページ／図*、＿＿＿＿ 付けで国際予備審査機関が受理したもの
第＿＿＿＿ ページ／図*、＿＿＿＿ 付けで国際予備審査機関が受理したもの

☐ 配列表又は関連するテーブル
配列表に関する補充欄を参照すること。

3．☑ 補正により、下記の書類が削除された。

☐ 明細書 第＿＿＿＿ ページ
☑ 請求の範囲 第 4 項
☐ 図面 第＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿

4．☐ この報告は、補充欄に示したように、この報告に添付されかつ以下に示した補正が出願時における開示の範囲を超えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)）

☐ 明細書 第＿＿＿＿ ページ
☐ 請求の範囲 第＿＿＿＿ 項
☐ 図面 第＿＿＿＿ ページ／図
☐ 配列表（具体的に記載すること）＿＿＿＿
☐ 配列表に関連するテーブル（具体的に記載すること）＿＿＿＿

＊ 4．に該当する場合、その用紙に "superseded" と記入されることがある。

特許性に関する国際予備報告

国際出願番号 ＰＣＴ／ＪＰ２００５／００１４３７

第Ⅴ欄　新規性、進歩性又は産業上の利用可能性についての法第12条（ＰＣＴ35条(2)）に定める見解、それを裏付ける文献及び説明

１．　見解

新規性（Ｎ）	請求の範囲	2, 3, 5-10	有
	請求の範囲	1	無
進歩性（ＩＳ）	請求の範囲	2, 3, 5-10	有
	請求の範囲	1	無
産業上の利用可能性（ＩＡ）	請求の範囲	1-3, 5-10	有
	請求の範囲		無

２．　文献及び説明（ＰＣＴ規則70.7）

文献１：JP 2000-207483 A（日本電信電話株式会社）2000.07.28，段落【0041】－【0049】，図７

文献２：JP 2002-237810 A（日本電気株式会社）2002.08.23，段落【0001】－【0009】，図10

文献３：D. Beaver、S. Micali、and P. Rogaway, "The round complexity of secure protocols", Annual ACM Symposium on Theory of Computing 22, 1990.05.14, p.503-513

文献４：Y. Ishai and E. Kushilevitz, "Randomizing Polynomials: A new Representation with Applications to Round-Efficient Secure Computation", IEEE Symposium on Foundations of Computer Science 2000, 2001.01.22, p.294-304

請求の範囲１
出願人が答弁書で認めた通り、文献１に記載された発明は請求の範囲１に係る発明の特別な場合である。
したがって、文献１に記載された発明は請求の範囲１に係る発明に含まれる。

請求の範囲２，３，５－１０
請求の範囲２，３，５－１０に係る発明は、国際調査報告で引用されたいずれの文献にも記載されておらず、当業者にとって自明なものでもない。

請求の範囲

１．（補正後） 複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

各周の計算と、

出力処理とからなり、

前記入力処理では、前記複数の計算装置に、与えられた関数に対応する回路の構成を記述する情報と、前記回路への入力ビットとが入力され、

前記各周の計算では、まず一台の前記計算装置が計算を行い、その計算結果を他の前記計算装置のうち一台に送り、次にその計算結果を受け取った前記前記計算装置がその次の計算を行う、というとように一台ずつ順に計算を行ってその計算結果を次の一台に回し、全ての前記計算装置が一度ずつ計算が終わったら、最後に計算をした計算装置が最初に計算をした計算装置に計算結果を送り、以後何度も、一台ずつ順に計算を行ってその計算結果を次の一台に回すという各周の計算を繰り返す事を特徴とする計算方法。

２．（補正後） 複数の計算装置を含む機器を用いて与えられた関数の値を計算する方法であって、

入力処理と、

ElGamal 暗号文準備処理と、

逐次置換再暗号処理と、

結果出力処理とからなり、

前記入力処理は、

前記複数の計算装置に複数のゲートから構成された回路の情報及び前記複数の計算装置に関する情報が入力される、情報入力ステップと、関数の入力データを複数に計算装置の個数に分散したデータである複数の部分データを、それぞれの計算装置にそれぞれ一つずつ入力する分散入力ステップと、からなり、

前記 ElGamal 暗号文準備処理は、少なくとも一つの計算装置が、与えられた関

数を実現する回路のゲートに対応した ElGamal 暗号文の集合を生成する ElGamal 暗号文準備ステップとからなり、

前記逐次置換再暗号処理は、

置換再暗号処理を各計算装置が順番に行う処理で、前記置換再暗号処理は、順番が回ってきた計算装置が、一つ前の順番に対応する計算装置から ElGamal 暗号文の集合を受け取る暗号文取得ステップと、

前記暗号文取得ステップにて受け取った暗号文の集合を順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化ステップと、

前記暗号文の置換と再暗号化ステップで生成したデータを、少なくとも次の順番の計算装置に公開するステップと、からなり、

前記結果出力処理は、

前記逐次置換再暗号処理で生成された暗号文の一部を復号あるいは部分復号する部分復号ステップと、

前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文を復号する復号ステップと、

前記復号ステップで復号されたデータと、前記部分復号ステップで部分復号されたデータを用いて、回路の出力を評価する回路の評価ステップとからなり、

前記各ゲートに対応する ElGamal 暗号文の集合は、前記各計算装置が各ゲートに対応して生成した秘密鍵の ElGamal 暗号文の集合であり、

前記 ElGamal 暗号文を生成するのに用いた公開鍵は、このゲートに入力される二つの信号を生成するゲートに対応する公開鍵の和であり、

それらは、出力１に対応する暗号文と、出力０に対応する暗号文の組みが、計算する論理式に合わせて複数準備されていて、

逐次暗号化処理は、前記暗号文を再暗号化して置換する処理で、１と０に対応する暗号文がそれぞれ入れ替わる置換のみを行ない、１と１に対応する暗号文がそれぞれ入れ替わる様な置換を行なわない処理であり、

最終的な復号結果は、１と０のどちらか一方の暗号文のみ復号する処理であることを特徴とする計算方法。

３．（補正後）　複数の計算装置と、

複数の計算装置と通信する手段と、

入力処理手段と、

ElGamal 暗号文準備手段と、

置換再暗号処理手段と、

結果出力処理手段と、からなる関数を評価する計算システムであって、

前記入力処理手段は、出力を求めたい回路の情報と、前記複数の計算装置に関する情報と、前記複数の計算装置がそれぞれ前記回路の入力のどの部分を所持しているかという情報と、を入力し、

前記 ElGamal 暗号文準備処理手段は、与えられた関数を実現する回路のゲート

に対応したElGamal暗号文の集合を生成するElGamal暗号文を準備し、

前記置換再暗号処理手段は、

順番が回ってきた計算装置が、一つ前の順番に対応する計算装置からElGamal暗号文の集合を受け取る暗号文取得手段と、

前記暗号文取得手段により受け取られた暗号文の集合の順序を入れ替えて置換し、それらを再暗号化する暗号文の置換と再暗号化手段と、

前記暗号文の置換と再暗号化手段を用いて生成したデータを、少なくとも次の順番の計算装置に公開する手段と、からなり、

前記結果出力手段は、

置換再暗号処理手段で生成された暗号文の一部を復号あるいは部分復号する部分復号手段と、

前記前記逐次置換再暗号処理で生成された暗号文の中で前記回路の入力に対応するデータを暗号化している暗号文の自分に関する暗号化を復号する復号手段と、

前記複数の計算機が前記復号手段で復号したデータと前記複数の計算機が前記部分復号手段で部分復号されたデータを用いて回路の出力を評価する回路の評価手段とからなり、

前記各ゲートに対応するElGamal暗号文の集合は、前記各計算装置が各ゲートに対応して生成した秘密鍵のElGamal暗号文の集合であり、

前記ElGamal暗号文を生成するのに用いた公開鍵は、このゲートに入力される二つの信号を生成するゲートに対応する公開鍵の和であり、

それらは、出力1に対応する暗号文と、出力0に対応する暗号文の組みが、計算する論理式に合わせて複数準備されていて、

逐次暗号化処理は、前記暗号文を再暗号化して置換する処理で、1と0に対応する暗号文がそれぞれ入れ替わる置換のみを行ない、1と1に対応する暗号文がそれぞれ入れ替わる様な置換を行なわない処理であり、

最終的な復号結果は、1と0のどちらか一方の暗号文のみ復号する処理であることを特徴とする計算システム。

4. （削除）

５．　前記請求項２に記載された計算方法において、

前記入力処理として、各計算装置に ElGamal 暗号方式の領域変数を入力するステップが行なわれ、

前記 ElGamal 暗号文準備処理として、各前記計算装置が、各前記回路の各ゲートに対応して、ElGamal 暗号文の秘密鍵を生成するゲート秘密鍵生成ステップが行